This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12)UK Patent (19)GB (11)2 369 019 (13)B

(45) Date of publication: 24.07.2002

(54) Title of the invention: Method for carrying out real-time backup communication of IP communication

(51) Int Cl[7]: **H04M** 7/00

(21) Application No: **0202535.1**

(22) Date of Filing: **09.08.2000**

Date Lodged: **04.02.2002**

(30) Priority Data:
(31) **11224868** (32) **09.08.1999** (33) **JP**

(62) Divided from Application No **0019611.3** under Section 15(4) of the Patents Act 1977

(43) Date A Publication: **15.05.2002**

(52) UK CL (Edition T):
H4P PEE PENE PPD
H4K KOA

(56) Documents Cited:
EP 1035719 A2
EP 0920176 A2
EP 0910201 A2
WO 99/28979 A2
JP 110308345 A
US 5898668 A

(58) Field of Search:
As for published application 2369019 A *viz:*
UK CL (Edition T) **H4P** PEE PENE PENX PEX PPD
INT CL[7] **H04L** 1/12 1/14 1/20 1/22 12/66 29/06, **H04M** 3/22 3/42 7/00
Online: WPI, EPODOC, JAPIO
updated as appropriate

(72) Inventor(s):
Mitsuo Suzuki

(73) Proprietor(s):
NEC Corporation
(Incorporated in Japan)
7-1 Shiba 5-chome, Minato-ku, Tokyo 108, Japan

(74) Agent and/or Address for Service:
Mathys & Squire
100 Grays Inn Road, LONDON, WC1X 8AL, United Kingdom

2369019

Fig. 1

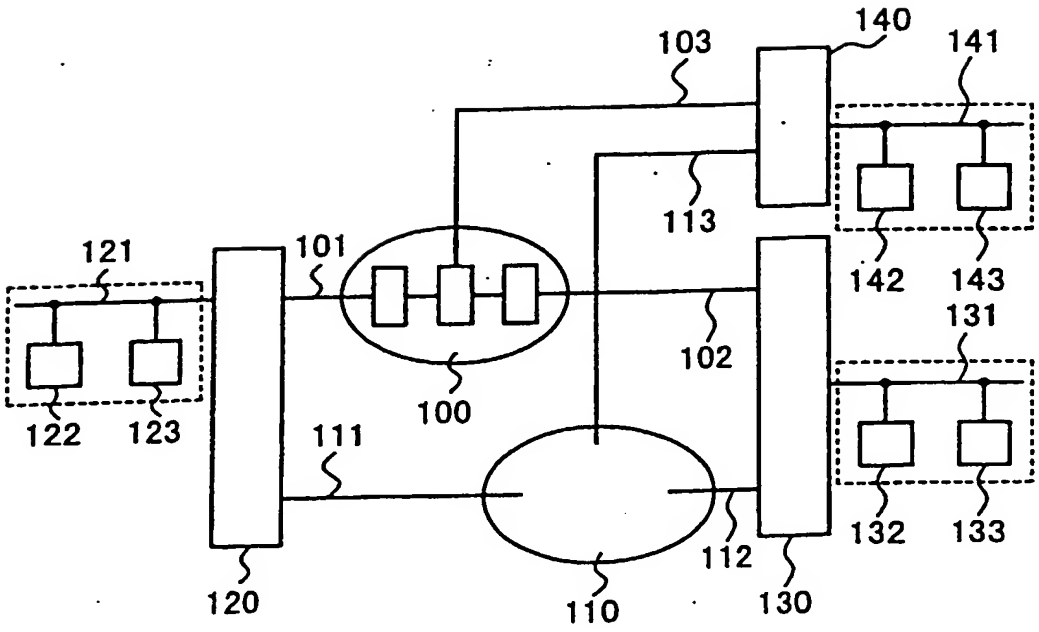
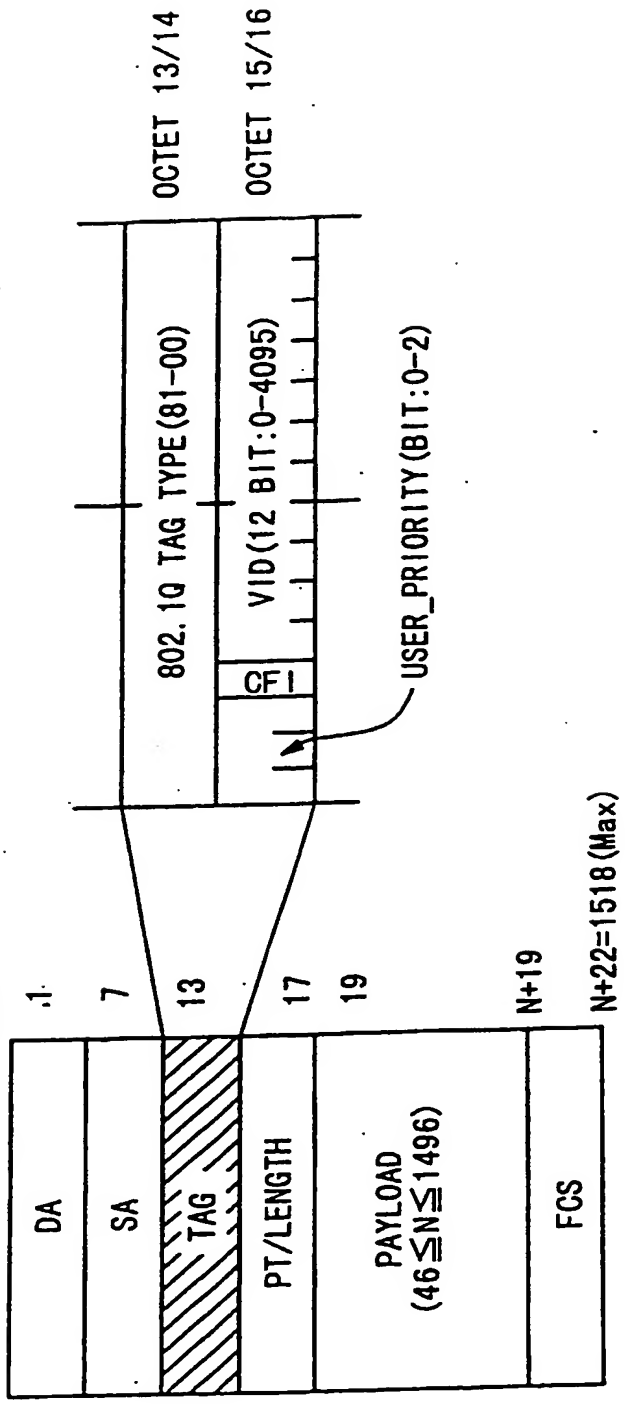


Fig. 2

ETHERNET FRAME WITH TAG OF IEEE 802.1Q



DA:DESTINATION ADDRESS

SA:SOURCE ADDRESS

PT:PAYLOAD TYPE

Fig. 3

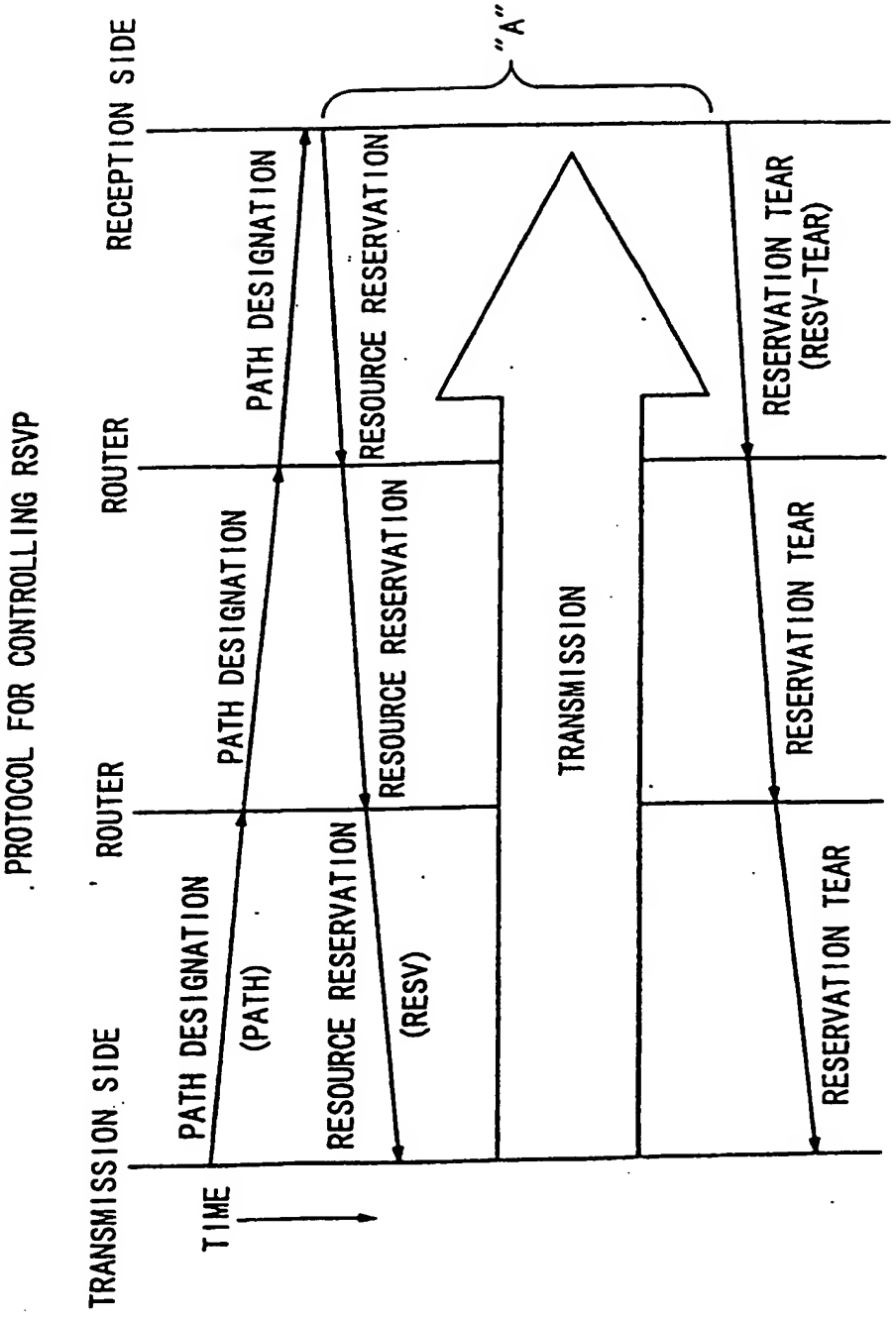

PROTOCOL FOR CONTROLLING RSVP
TRANSMISSION SIDE
ROUTER
ROUTER
RECEPTION SIDE
TIME
PATH DESIGNATION (PATH)
RESOURCE RESERVATION (RESV)
PATH DESIGNATION
RESOURCE RESERVATION
PATH DESIGNATION
RESOURCE RESERVATION
"A"
TRANSMISSION
RESERVATION TEAR
RESERVATION TEAR
RESERVATION TEAR (RESV-TEAR)

Fig. 4

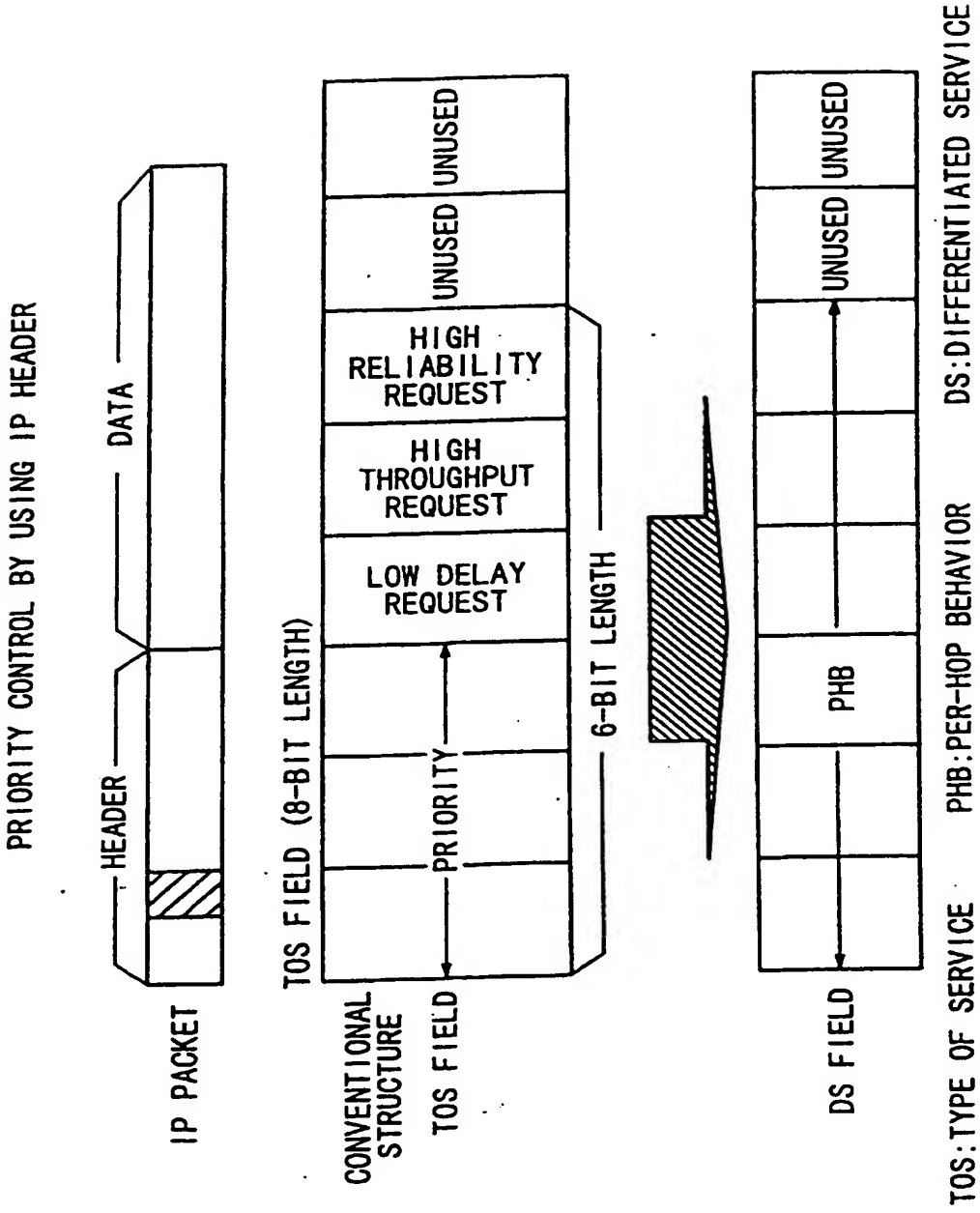

PRIORITY CONTROL BY USING IP HEADER
HEADER
DATA
IP PACKET
TOS FIELD (8-BIT LENGTH)
PRIORITY
LOW DELAY REQUEST
HIGH THROUGHPUT REQUEST
HIGH RELIABILITY REQUEST
UNUSED
UNUSED
6-BIT LENGTH
CONVENTIONAL STRUCTURE
TOS FIELD
PHB
UNUSED
UNUSED
DS FIELD
TOS:TYPE OF SERVICE
PHB:PER-HOP BEHAVIOR
DS:DIFFERENTIATED SERVICE

Fig. 5

IP DATAGRAM FORMAT AND FUNCTION

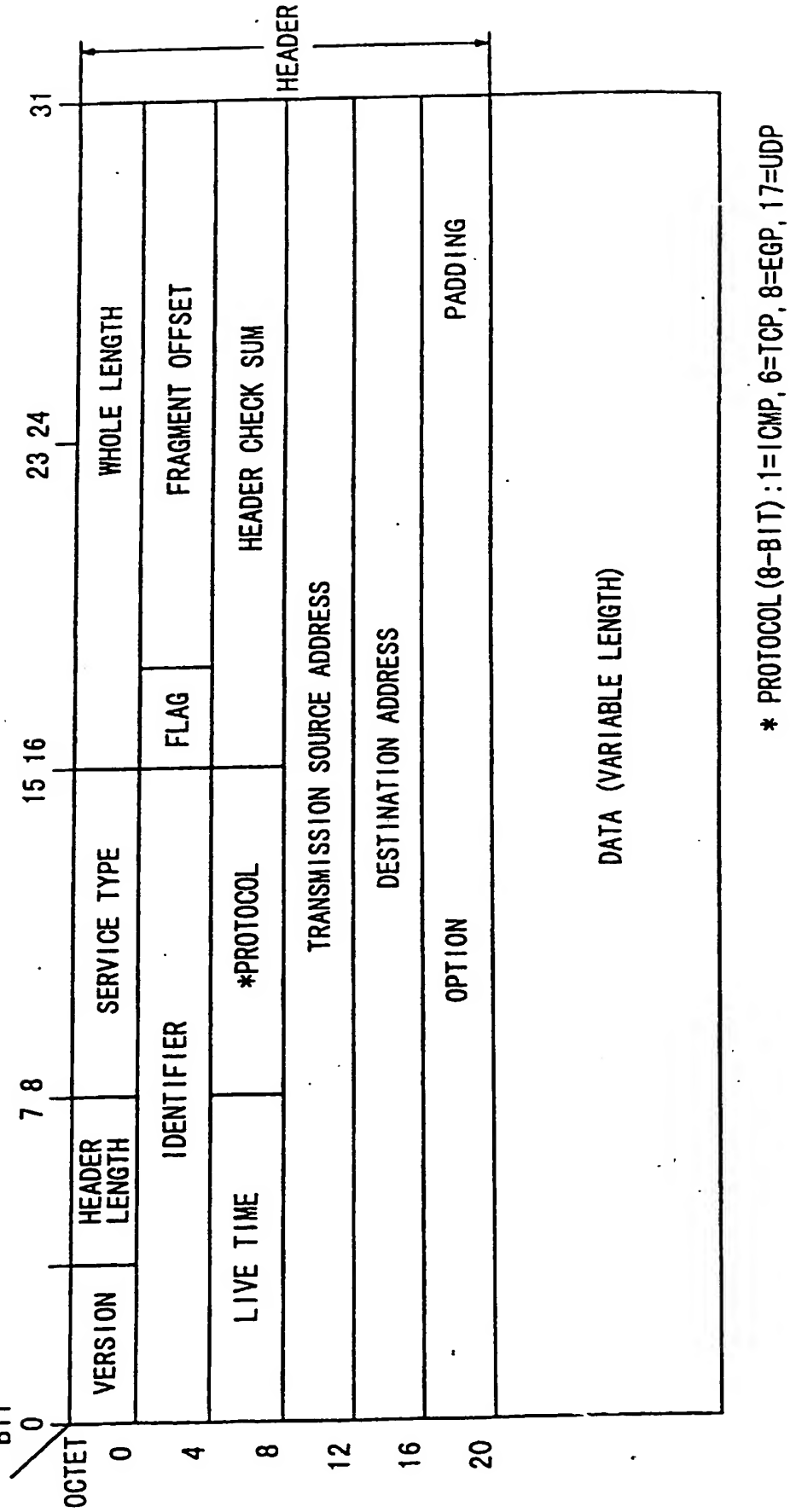


Fig. 6

KIND OF ICPM MESSAGE

TYPE	CONTENT
00	ECHO REPLY
03	DESTINATION UNREACHABLE
04	SOURCE QUENCH
05	REDIRECT
08	ECHO REQUEST
11	TIME EXCEEDED
12	PARAMETER PROBLEM
13	TIMESTAMP REQUEST
14	TIMESTAMP REPLY
15	INFORMATION REQUEST
16	INFORMATION REPLY
17	ADDRESS MASK REQUEST
18	ADDRESS MASK REPLY

Fig. 7

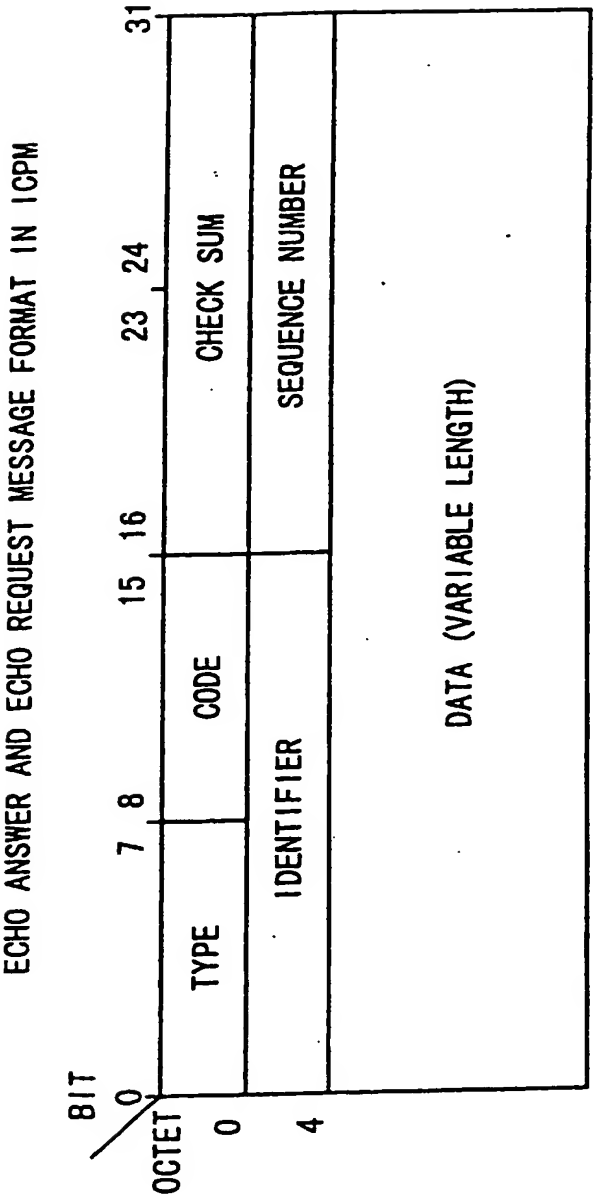

ECHO ANSWER AND ECHO REQUEST MESSAGE FORMAT IN ICPM
BIT
0
7 8
15 16
23 24
31
OCTET
0
4
TYPE
CODE
CHECK SUM
IDENTIFIER
SEQUENCE NUMBER
DATA (VARIABLE LENGTH)

Fig. 8

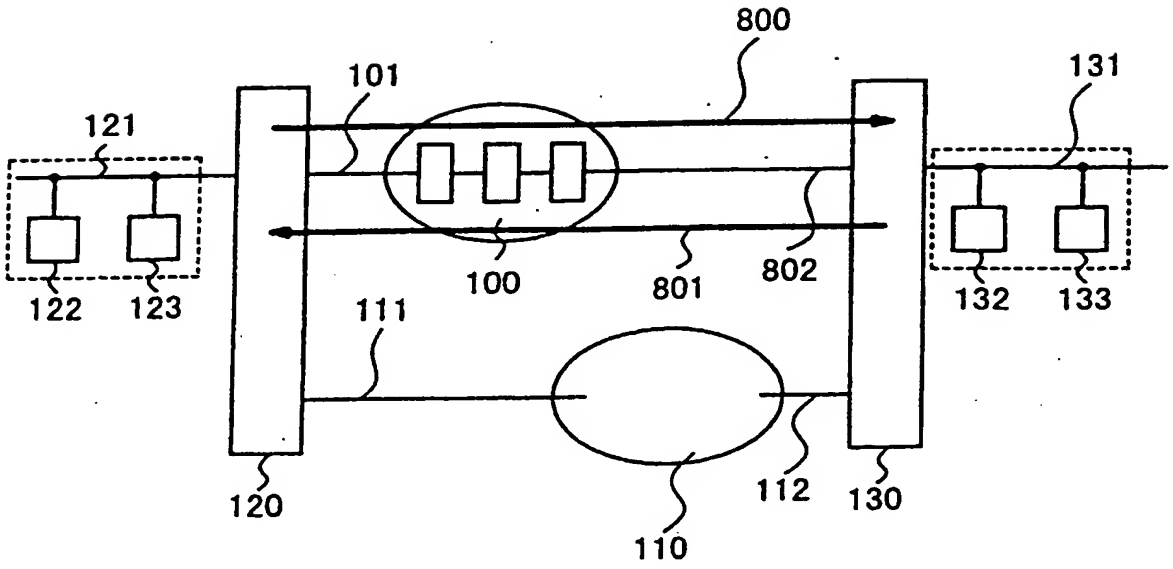
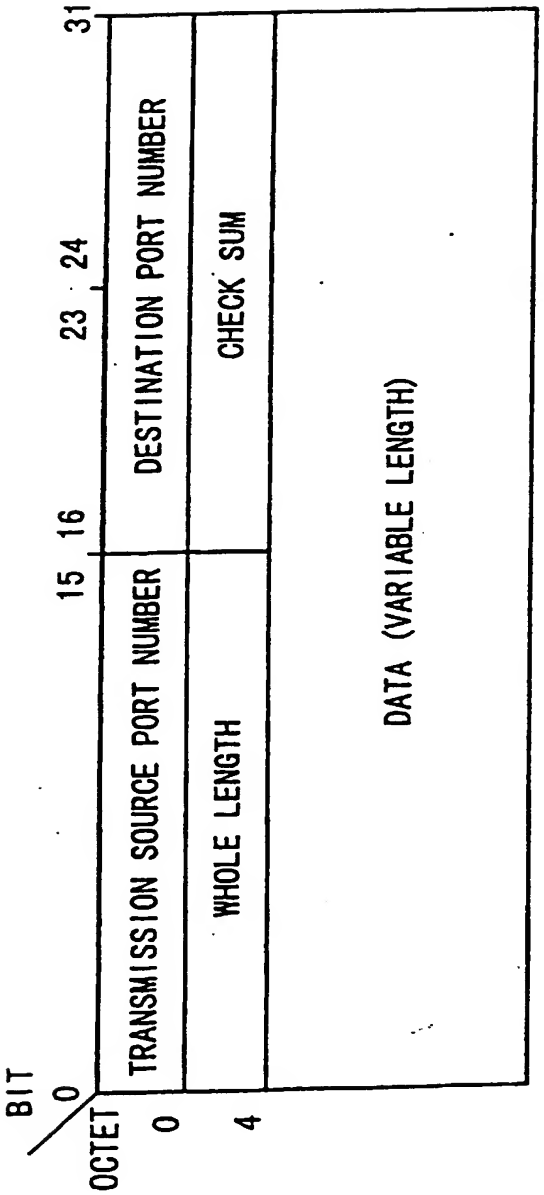


Fig. 9


UDP MESSAGE FORMAT
BIT
0
15 16
23 24
31
OCTET
0
4
TRANSMISSION SOURCE PORT NUMBER
DESTINATION PORT NUMBER
WHOLE LENGTH
CHECK SUM
DATA (VARIABLE LENGTH)

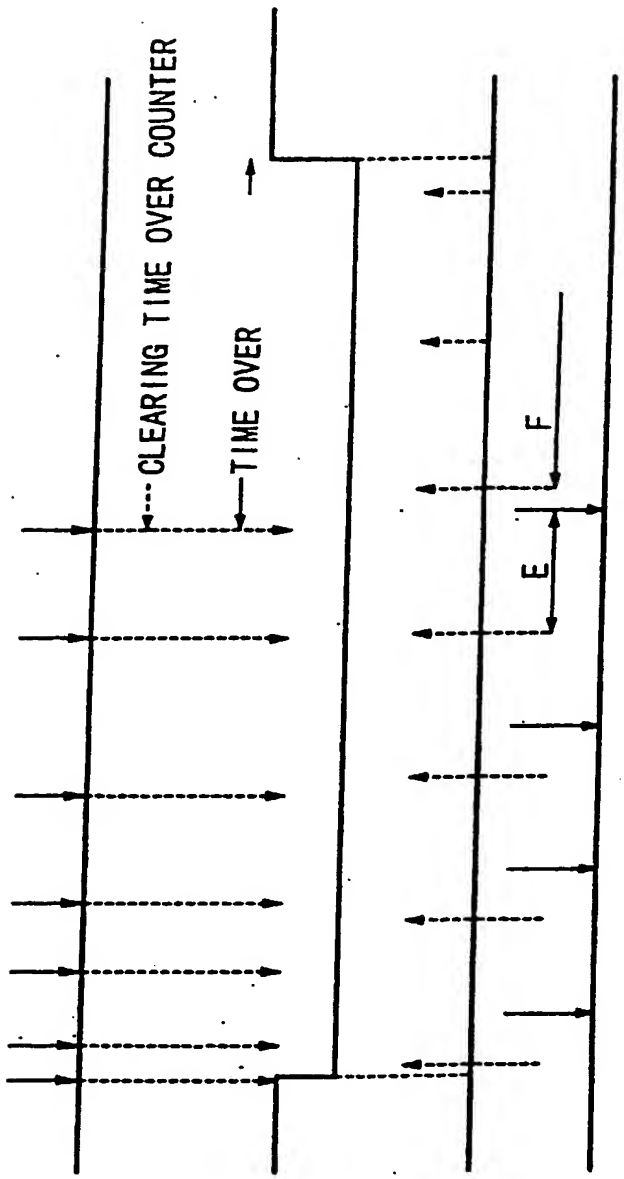


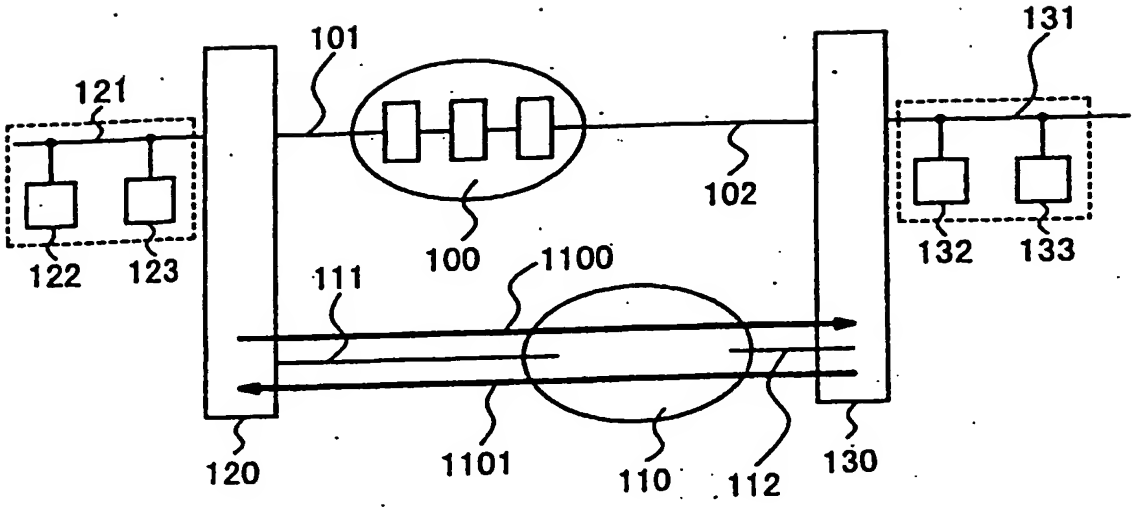
Fig. 10A

Fig. 10B

Fig. 10C

Fig. 10D

Fig. 11


101
121
131
102
100
122
123
132
133
111
1100
120
1101
110
112
130

METHOD FOR CARRYING OUT REAL-TIME BACKUP COMMUNICATION OF IP COMMUNICATION

Background of the Invention

1. Field of the Invention

The present invention relates to a method for carrying out real-time backup communication of Internet Protocol (referred to as "IP" hereinafter) communication. More particularly, the present invention relates to a method for carrying out real-time backup communication of IP communication using a public network.

2. Description of the Related Art

In recent years, real-time communication has begun to be used for data such as voice and animation of the Internet, Intranet and Extranet (hereafter referred to as "Internet network" or "IP network"). Activities of IETF standardization have become active with regard to the QoS (Quality of Security) control for securing the quality of real-time communication as much as possible. The main items among them are as follows:

(1) RSVP (ReSource reserVation Protocol): resource reservation protocol

(2) RTP (Real-time Transport Protocol)/RTCP (Real-time Transport Control Protocol): real-time communication control protocol

(3) DiffServe (Differentiated Service): priority

control using IP header

(4) RTSP (Real-time Transport Streaming Protocol): stream data Control Protocol

Those QoS controls alone can not carry out the real-time communication that is stable on the Internet network. For example, a real-time communication call such as voice data, animation data and the like, from a transmission side node causes an error at a reception side node because of troubles of a network and a node connected to the Internet network. A real-time communication that is communication in a UDP (User Datagram Protocol) procedure that does not carry out a re-transmission control does not have means for detecting the trouble of the Internet network on the node side. Thus, it is impossible to judge whether the trouble results from an opposite node trouble or a network trouble.

Under such situation, a maintenance technician having a high ability who firstly detects the network trouble based on a communication error report from a user uses a method for transmitting an echo request message between nodes, and firstly checking the error based on an absence of a reply with regard to an echo answer message, and manually switching to a public network such as INS and the like, to thereby carry out a backup switching operation. The specification of the trouble cause necessary for the execution of this

method requires high maintenance skill of the maintenance technician. Moreover, the maintenance technician having such high skill needs to carry out a large number of processes to specify the network trouble and the communication trouble. Moreover, it takes a long time to carry out a series of trouble analyses, from the user request to the manual operations, by the maintenance technician having the high maintenance skill, resulting in a large drop of related services.

Particularly associated with the down-sizing and flatting (horizontalizing) of the network resulting from the IP network in recent years, it is economically difficult to station the maintainers having the special and high skills for many respective small networks existing in an enterprise. So, a system begins to be required in which even a maintainer holding another low typical service, namely, an amateurish maintainer assigned in each department, can quickly specify the trouble reasons. In other words, the desire to establish a mechanism for economically insuring a reliability of the IP network has become popular in which the drop of the communication quality caused by the network trouble and the network delay time in the Internet network that is very economic, although being low in reliability and quality, can be monitored on a user-

equipment side by using a cheap method, and it is possible to carry out a stable continuous communication of a real-time communication call.

A related technique is disclosed in Japanese Laid-Open Patent Application (JP-A-Heisei, 10-224408) as "COMMUNICATION SYSTEM". First and second communication apparatuses in this communication system have switching means, data-format converting means and switching control means. The switching means contains a plurality of communication lines including a call path highway provided with a plurality of channels, which are connected to public networks, dedicated lines and inner terminals. The data format converting means connects a computer network and the call path highway, and converts a format of a transmission data between the computer network and the call path highway, and also transmits and receives data to and from a destination communication apparatus through the computer network. The switching control means transmits and receives call control information to and from the destination communication apparatus through the computer network, and also controls the switching means and the data format converting means so as to establish the connection using the computer network, in accordance with the data kinds at a terminal on a transmission side and a terminal on a reception destination. According to this

communication system, a mutual communication can be done between the terminals, in which the data kinds are different from each other, by using the computer network without a manual operation.

Japanese Laid-Open Patent Application (JP-A-Heisei, 10-65737) discloses "SUBSTITUTE SERVER APPARATUS AND SERVER APPARATUS". The substitute server apparatus contains: means for carrying out a PPP connection through a public network between a network and the server apparatus, by dynamically assigning an IP address in accordance with a specified server apparatus name and a telephone number in a corresponding public network, between the network and the server apparatus; and means for accessing the server apparatus by using the dynamically-assigned IP address. Accordingly, with regard to the server apparatus to be connected to the network managed by the IP address through the public network, even if it is not connected to the network at a time of the communication request, and if even further the IP address is not determined, it is possible to connect the server apparatus to the network and dynamically assign the IP address and further communicate with the dynamically-assigned IP address based on the server apparatus name.

Moreover, Japanese Laid-Open Patent Application (JP-A-Heisei, 9-130429) discloses "COMMUNICATION SYSTEM". In this communication system, a line/packet

converter is connected between a computer network and a call path highway in a private switch. A computer terminal transmits and receives a call control packet to and from the private switch through the computer network. The line/packet converter converts a format of a transmission data between the computer network and the call path highway. Accordingly, it is possible to connect the computer network, a subscriber line, and an extension line so that the computer terminal can communicate with another communication terminal through a public network and an extension line network.

Summary of the Invention

Therefore, an object of the preferred embodiment of the present invention is to provide a method for carrying out real-time backup communication of IP communication, which can protect a drop in communication quality caused by network delay time and network trouble in an Internet network that is very economic, by using a cheap and simple method.

Another object of the preferred embodiment of the present invention is to provide a method for carrying out real-time backup communication of IP communication, which can attain a technique for economically insuring a reliability of an Internet network by executing real-time communication stably and continuously.

Means for solving the above-mentioned problems are explained as follows. A number, a symbol or the like, together with parentheses "()", is given to a technical item appearing in the explanation. The number, the symbol or the like coincides with a reference number, a reference symbol or the like given to a technical item constituting at least one embodiment or a example among a plurality of embodiments or a plurality of examples in the present invention, especially a technical item illustrated in a drawing corresponding to the embodiment or the example. Such reference numbers and reference symbols evidently denote a corresponding relation between the technical item noted in the claims and the technical item in the embodiment or the example. Such corresponding relation does not imply the interpretation that the technical item noted in the claims is not limited to the technical item in the embodiment or the example.

One form of the present invention is a method for carrying out a real-time backup communication of Internet Protocol (IP) communication, which method includes steps of: detecting when the duration of a delay time, extending from transmission of an echo request message from a transmission-side node to reception of an echo answer message at the transmission-side node, exceeds a predetermined allowed time

interval indicative of secured quality of a real-time communication on an IP network; bypassing, depending on a result of the detecting step, from the IP network to a public network, a communication call of the real-time communication performed between the transmission-side node and the reception-side node; and, bypassing a new communication call that occurs while the bypassing operation of the communication call to the public network is being performed.

The one form of the method may further include the step of judging, after the detected duration of the delay time has exceeded the predetermined allowed time, whether the IP network or the reception-side node is abnormal.

The one form of the method may further include the step of detecting an error in a real-time communication on the public network through which the transmission-side node and the reception-side node are connected, the further step including detecting, on the public network, a duration of a delay time from a transmission of an echo request message to a reception of an echo answer message between the transmission-side node and the reception-side node.

The one form of the method may further include the step of detecting an error in a real-time communication on the public network through which the transmission-side node and the reception-side node are connected, the further step including judging, after the detected duration of a delay time

for response to an echo request message has exceeded a predetermined allowed time interval for response to the message, whether the public network is abnormal.

The one form of the method may further include the step of judging whether it is the reception-side node that is abnormal or the IP network that is abnormal, the judgment being based on measuring the delay time for an echo signal passed along the public network after the communication call has been bypassed to the public network from the IP network.

Internet Control Message Protocol (ICMP) may be used in the transmission of the echo request message and reception of the echo answer message.

Another form of the present invention is a system configured to effect the method of the above-described first form of the invention.

Brief Description Of The Drawings

Preferred features of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 shows a circuit block diagram used in an embodiment of a method for carrying out a real-time backup communication of IP communication according to the present invention;

Fig. 2 shows a data configuration of Ethernet

Frame with Tag of IEEE 802.1Q;

Fig. 3 shows a time chart representing a method for controlling RSVP;

Fig. 4 shows a data configuration indicating a field format with regard to a priority control in a conventional technique and the present invention;

Fig. 5 shows an IP datagram format and function;

Fig. 6 shows a kind of ICMP message;

Fig. 7 shows an echo answer message and an echo request message format in ICMP;

Fig. 8 is a circuit block diagram showing a part of operation signals of Fig. 1;

Fig. 9 shows a data configuration indicating a message format of UDP;

Figs. 10A to 10D show a timing chart of a signal flow of detecting a delay of an answer; and,

Fig. 11 shows a circuit block diagram of a well-known apparatus.

Description of the Preferred Embodiments

Coinciding with and corresponding to the drawings, in an embodiment of a method for carrying out a real-time backup communication of IP communication according to the present invention, a public (line) network 110 is provided together with an IP network 100. As shown in Fig. 1, a transmission side node 120 is connected through an IP-side first

connection interface 101 to the IP network 100. The IP network 100 is connected through an IP-side second connection interface 102 and an IP-side third connection interface 103 to a reception-side first node 130 and a reception-side second node 140, respectively.

The transmission-side node 120 is connected through a public-network-side first connection interface 111 to the public network 110. The public network 110 is connected through a public-network-side second connection interface 112 and a public-network-side third connection interface 113 to the reception-side first node 130 and the reception-side second node 140, respectively.

A transmission-side voice terminal 122 and a transmission-side animation terminal 123 are connected to a transmission-side LAN 121. The transmission-side LAN 121 is connected to the transmission-side node 120. A first reception-side voice terminal 132 and a first reception-side animation terminal 133 are connected to a first reception-side LAN 131. The reception-side LAN 131 is connected to the reception-side first node 130. A second reception-side voice terminal 142 and a second reception-side animation terminal 143 are connected to a second reception-side LAN 141. The second reception-side LAN 141 is connected to the reception-side second node 140.

In the real-time communication such as a multi-media communication in which voice data and animation data are transmitted and received, TCP (Transmission Control Protocol) is not used, because the TCP brings about a delay by a message re-transmission when a communication error is induced. The TCP is defined by setting a *protocol field (refer to Fig. 5) to "06" in Hexadecimal Number. Then, UDP (User Datagram Protocol) is used, because the UDP does not bring about the re-transmission even if an error is induced. The UDP is defined by setting a *protocol field (refer to Fig. 5) to "17" in Hexadecimal Number.

The voice terminal 122 and the animation terminal 123 which are connected to the LAN 121 are operated in accordance with "Ethernet Frame with Tag of IEEE 802.1Q" shown in Fig. 2. When the voice and animation having a high real-time property is transferred, a three-bit User Priority field formed in a Tag field of this Ethernet Frame is set to a value having the highest priority.

The IP network 100 has the configuration to enable the controls such as RSVP (ReSource reserVation Protocol) shown in Fig. 3, DiffServe (Differentiated Services), a QoS setting at IP over ATM, and the like. In a section "A" of Fig. 3, a resource reservation message is periodically sent out and a securing of resources is continued. RSVP is used for a control,

e.g. a signaling control for interpolating a network layer (IP), to enable QoS (Band Security) for a voice and animation having a high real-time property and is a protocol to reserve a network resource in a single direction under an instruction on a reception side for receiving information. DiffServe is a priority control service based on a contract between a user and an ISP (Internet Service Provider). To realize a priority control by using IP header, a TOS (Type Of Service) field (8-bit length) in an IP header which is shown in Fig. 4 and was not almost used, is again defined as a Differentiated Services field. The higher 6 bits of the Differentiated Services field is named as a PHB (Per-Hop-Behavior) field and three bits among the higher 6 bits can be used to set a six-level priority.

Moreover, the IP network 100 is provided with an RTP/RTCP (Real-time Transport Protocol / Real-time Transport Control Protocol) and an RTSP (Real-time Transport Streaming Protocol). The RTP/RTCP is a real-time communication control protocol for carrying out a synchronous control between media and a control of a reproduction speed on a reception side, by giving a sequence number and physical time information for each message to a header from a transmission-side terminal, in order to improve real-time communication quality between the terminals, namely, between an application

and a transport layer, independently of a network. Also, the RTSP (Real-time Transport Streaming Protocol) is a stream data control protocol for dynamically informing a communication speed and a display quality, such as a resolution and a number of animation frames per second from the reception side, to the transmission side.

It may be considered that a real-time telephone communication is done between the transmission-side voice terminal 122 on the LAN 121 and the first reception-side voice terminal 132 on the first reception-side LAN 131, through the IP network 100. The transmission-side voice terminal 122 sets DA (Destination Address) corresponding to the first reception-side voice terminal 132 for "Ethernet Frame with IEEE 802.1Q Tag" shown in Fig. 2, and sets the highest priority bit in the User Priority field of the Tag, and then transmits to the transmission-side node 120.

The transmission-side node 120 converts the DA (Destination Address) on the transmission-side LAN 121 into an IP number (IP number of the reception-side first node 130) corresponding to the first reception-side voice terminal 132, and simultaneously detects the highest priority bit in the User Priority field, and then maps to the QoS control (RSVP, DiffServe or IP over ATM) of the IP network 100.

As an example, a case is described in which the transmission-side node 120 sets the highest priority bit to the three bits in the PHB field of the IP header in the DiffServe of Fig. 4 and then transmits to the IP network as the QoS control. As a result, as shown in Fig. 1, it is possible to reserve the real-time communication in which the QoS is reserved up to the transmission-side voice terminal 122 - the transmission-side LAN 121 - the transmission-side node 120 - the IP-side first connection interface 101 - the IP network 100 - the IP-side second connection interface 102 - the reception-side first node 130. Moreover, the reception-side first node 130 sets the highest-priority bit to the User Priority field in the Tag and the DA corresponding to the first reception-side voice terminal 132 into "Ethernet Frame with 802.1Q Tag" shown in Fig. 2, and transmits it from the internal LAN 131 to the first reception-side voice terminal 132. Thus, it is possible to attain the real-time communication based on the QoS control through the IP network 100 between the transmission-side voice terminal 122 and the first reception-side voice terminal 132.

If 8 bits in a *protocol shown in Fig. 5 is "01" in Hexadecimal Number, ICMP (Internet Control Message Protocol) is specified as shown in Figs. 6 and 7. If 8 bits of "type" shown in Figs. 6 and 7, which

represents a message type, are "08" in Hexadecimal Number, this indicates an echo request, and if "00", this indicates an echo answer. An echo function including the echo request and the echo answer is used when it is checked whether or not a host or a node connected to the IP network 100 is active. Thus, if a certain host or node transmits an echo request of a message type "08", a specified host or node repeats an echo answer of a message type "00", when it is in the state which can respond. The operational check using such an echo is frequently done. The echo request is transmitted by using a utility program typically referred to as a ping.

As shown in Fig. 8, the transmission-side node 120 sets an IP address number of the transmission-side node 120 to a transmission-source address field shown in Fig. 5, sets an IP address number of the node 130 into a destination address field, sets "01" in Hexadecimal Number (ICMP) to the *protocol, and further sets "08" in Hexadecimal Number (the echo request shown in Fig. 6) to the message-type field shown in Fig. 7, and then transmits an echo request message 800 of Fig. 8, in which a test data for a loop back is set to a data (variable-length) field of Fig. 7, through the IP network 100 to the reception-side first node 130.

The reception-side first node 130, when

receiving the echo request message 800 of Fig. 8, sets the IP address number of the reception-side first node 130 into the transmission-source address field of Fig. 5, sets the IP address number of the transmission-side node 120 into the destination address field, sets "01" in Hexadecimal Number (ICMP) into the *protocol field, and further sets "00" in Hexadecimal Number (the echo answer of Fig. 6) into the message-type field of Fig. 7, and copies the test data for a loop back, which is written to a data field of the received echo request message 800 of Fig 8, to the data field (the variable length) in its original state, and then sends back to the transmission-side node 120 as an echo answer message 801 of Fig. 8. Thus, the transmission-side node 120 that is the transmission-source node can check the state of the transmission and reception of the data through the loop back test and also detect the troubles of a network and a node on a route in the transmission-side node 120 - the IP-side first connection interface 101 - the IP network 100 - the IP-side second connection interface 102 - the reception-side first node 130. Simultaneously, the transmission-side node 120 can check that the excellent quality of the real time telephone communication can be reserved if a round trip time until the reception of the echo answer message 801, sent back from the reception-side first node 130 after the transmission-side node 120

transmits the echo request message 800, is within a time capable of reserving quality of a real-time communication, for example, if it is within 150 msec defined by ITU-TG.114.

Under such precise conditions, when the transmission-side voice terminal 122 shown in Fig. 1 carries out the real-time communication with the first reception-side voice terminal 132 through the transmission-side LAN 121, the transmission-side node 120, the IP-side first connection interface 101, the IP network 100, the IP-side second connection interface 102, the reception-side first node 130 and the first reception-side LAN 131, the transmission-side node 120 receives the Ethernet frame with the Tag shown in Fig. 2 coming from the transmission-side LAN 121. Then, the highest priority detection of the QoS is done in accordance with the User Priority within the Tag. Accordingly, a conversion from the DA into the IP address number of the first reception-side voice terminal 132 is executed.

At the same time, as shown in Fig. 10A, a voice data packet coming from the transmission-side LAN 121 to the transmission-side node 120 causes a time-over counter for detecting a voice data packet disconnection shown in Fig. 10B to be cleared, and it is switched to a voice communication mode (L level). Here, Fig. 10A shows the voice data packet between the

voice terminal 122 → the LAN 121 → the node 120 in case of the real-time communication to the voice terminal 132 from the voice terminal 122. Also, Fig. 10B shows an output of the time over counter for a voice data packet disconnection detection between LAN 121 → node 120 (L level represents voice communication, H level represents non-voice communication).

After that, in order to reserve the real-time communication from the transmission-side LAN 121 to the transmission-side node 120, the time-over counter is cleared for each voice data packet, which always comes within a certain succeeding time, and the voice communication mode (L level) is continued.

Associated with the end of the voice communication, since the signal to clear the time-over counter does not issue, the time-over counter causes the time-over. Therefore, it is switched to a non-call mode (H level). The transmission-side node 120 sets the highest priority bit for the three bits in the PHB field of the IP header in the DiffServe shown in Fig. 4 as the QoS control, sets "17" in Hexadecimal Number (UDP) to the *protocol field of Fig. 5, sets the IP address number of the transmission-side node 120 accommodating the transmission-side voice terminal 122 to the transmission-source address field, sets the IP address number of the reception-side first node 130

accommodating the first reception-side voice terminal 132 to the destination address field, and copies voice data at a payload in the Ethernet frame with IEEE 802.1Q Tag shown in Fig. 2 to the data field (variable portion) of the UDP in the transport layer of Fig. 9, and then transmits through the IP network 100 to the reception-side first node 130. The reception-side first node 130 transmits this received voice data to the first reception-side voice terminal 132, by detecting a real-time communication call, namely, the QoS control request call, in accordance with a destination port number of the UDP of Fig. 9, namely, an application, and the priority bit of three bits in the PHB in the IP header of Fig. 4, and then setting the highest priority bit in the User Priority field in the Ethernet frame with IEEE 802.1Q Tag of Fig. 2 on the first reception-side LAN 131. As a result, the real-time communication securing the QoS can be done between the transmission-side voice terminal 122 and the first reception-side voice terminal 132.

At the same time, the transmission-side node 120, as the QoS control, sets the highest priority bit for the three bits in the PHB field of the IP header in the DiffServe of Fig. 4, sets "01" in Hexadecimal Number (ICMP) to the *protocol field of Fig. 5, sets the IP address number of the transmission-side voice

terminal 122 to the transmission-source address field, sets the IP address number of the first reception-side voice terminal 132 (the IP address number of the reception side first node 130) to the destination address field, sets "08" in Hexadecimal Number (echo request) to the message-type field of Fig. 7, and transmits the echo request message 800 of Fig. 8, in which the test data for loop back is set for the data field (variable length), through the IP network 100 to the reception-side first node 130.

After that, this echo request message 800 is periodically transmitted for each constant interval (period) shown in Fig. 10C, in the voice communication mode at which an output from the time-over counter is at the L level. Here, Fig. 10C represents a sending-out time range and a sending-out interval of the echo request message 800 of Fig. 8 in ICMP. The transmission-side node 120 detects whether or not the round trip time until the reception of the echo answer message 801 sent back from the reception-side first node 130 within the constant time in Fig. 10C is within a time in which the quality of the real-time communication can be reserved, by using the time-over counter shown in Fig. 10D. Here, Fig. 10D represents a delay time from the transmitting of Fig. 10C to the reception of the echo response message 801 of Fig. 8. In Fig. 10D, "E" represents a case of the occurrence

of the time over because the delay time from the transmitting of Fig. 10C to the reception of the echo response message 801 is large, and "F" represents a case of the occurrence of the time over because of being not received the echo response message 801. Then, it judges that the trouble results from the IP or the opposite node 130, if the echo answer message 801 after an elapse of the round trip time is not received as shown in E of Fig. 10D and if the echo answer message 801 is not replied as shown in F of Fig. 10D.

In this case, the transmission-side node 120 converts the IP address number of the first reception-side voice terminal 132 at the connection destination (the IP address number of the reception side first node 130) into a telephone number of the public network 110, and then reserves a backup bypass route up to the transmission-side node 120 - the public-network-side first connection interface 111 - the public network 110 - the public-network-side second connection interface 112 - the reception-side first node 130, through the public network connection based on a dialup. The transmission-side node 120 transmits an echo request message 1100 of Fig. 11 through the public network 110 after the backup-switch bypass operation, to the reception-side first node 130, and then judges that the IP network 100 is abnormal and

the reception-side first node 130 is normal if the echo answer message 1101 from the reception-side first node 130 is replied within an allowable time, and judges that the reception-side first node 130 is abnormal if the echo answer message 1101 is not replied. So, it can request an emergent treatment if detecting the trouble in the reception-side first node 130.

Moreover, in order to continuously monitor the normal conditions with regard to the reception-side first node 130 and the public network 110 through the communication route of the public network 110 during the real-time communication resulting from this backup bypass operation, this is designed such that the operations perfectly equal to those in the series of configurations shown in Figs. 8, 10 are also applied to a public network 110 in Fig. 11, namely, the echo request message 800 is replaced by an echo request message 1100 of Fig. 11, and the echo answer message 801 is replaced by an echo answer message 1101 of Fig. 11. For greater specificity, with reference to Figs. 10, 11 and the foregoing description related to Figs. 8, 10, the echo request message 1100 is periodically transmitted for each constant interval (period) shown in Fig. 10C. The transmission-side node 120 detects whether or not the the round trip time until the reception of the echo answer message

1101 sent back from the reception-side first node 130 within the constant time in Fig. 10C is within a time in which the quality of the real-time communication can be reserved, by using the time-over counter shown in Fig. 10D. Then, it judges that the trouble results from the public network or the opposite node 130, if the echo answer message 1101 after an elapse of the round trip time is not received as shown in E of Fig. 10D and if the echo answer message 1101 is not replied as shown in F of Fig. 10D.

At the same time, the transmission-side node 120, in order to monitor the normal recovery from the network congestion, in which the IP delay time caused by the IP network disconnection/abnormal trouble and the round trip time-over is equal to or longer than a specified time, changes the condition shown in Fig.

10B into the IP trouble (including the round trip time-over) condition between the transmission-side node 120 and the reception-side first node 130, namely, a condition that Fig. 10B is forcedly switched to the L level at the time of the network trouble, and periodically transmits the echo request message 800 for each constant interval (period) shown in Fig. 10C.

The transmission-side node 120, after the transmission of the echo request message 800 of Fig. 8, namely, Fig. 10C, detects whether or not the round trip time until the reception of the echo answer message 801 sent back from the reception-side first node 130 within the constant time is within the time in which the quality of the real-time communication can be reserved, by using the time-over counter in Fig. 10D, and then continues to receive the echo answer message 801 after an elapse of an allowable limit time of the round trip time as shown in E of Fig. 10D or monitor until the recovery of the continuously (stably) normal state after the current trouble condition that the echo answer message 801 is not replied as shown in F of Fig. 10D. That is, this implies the continuation of the monitor until the IP network 100 between the transmission-side node 120 and the reception-side first node 130 recovers the normal state, even after the completion of the communication through the backup bypass operation between the

transmission-side node 120 and the reception-side first node 130. The backup bypass operation through the public network 110 is done if a communication call to the reception-side first node 130 is newly-generated during the continuous monitor.

After the check of the recovery of the normally-stable state in the IP network 100, if the real-time communication is done through the public network 110 from the transmission-side node 120 to the reception-side first node 130, switching to the IP network 100 whose normal state is recovered enables the communication to be done further economically. In this case, when the recovery to the normally-stable state is detected, the IP trouble condition in Fig. 10B, namely, the forced L level condition in Fig. 10B implying the network trouble state is once cleared and returned back to the H level implying the initial state. So, at a time of a start of the communication call to the IP, the monitor of the trouble in the IP network 100 is designed to be done in accordance with a normal sequence from Fig. 10A. It is also natural that the switching from the public network 110 to the IP network 100 is quickly done when the IP network 100 recovers the normal state, and then the series of typical real-time communications is done through the IP network 100, as mentioned above.

In the above-mentioned embodiment, it is

described that the transmission-side node 120 is used as the calling side and the reception-side first node 130 is used as the called side. However, if the transmission-side node 120 is used as the called side and the reception-side first node 130 is used as the calling side, the transmission-side node 120 can know that the reception call is the real-time communication call, from the port number of the UDP, namely, the application number, or the highest priority setting of the DiffServe priority bit in the PHB field in the IP header of Fig. 4. So, the execution of the operations perfectly equal to the series of operations in Figs. 10A to 10D and the series of operations in the echo request message 1100 and the echo answer message 1101 with regard to Fig. 11 enables the monitor of the IP trouble having the symmetry between the nodes, the monitor of the allowable delay time, the quick detection of the trouble and the maintenance.

In the above-mentioned explanation, the IP is described as the Internet network, for the purpose of easy explanation. However, it can include the intra-network and the extra-network. The real-time communication in the IP in which the QoS is secured is described in the above-mentioned explanation. However, it is possible to configure by using the currently-popular IP (Internet) network that is the best effort in which the QoS is not secured. So, the delay time

is monitored by monitoring the round trip time. Then, if it exceeds the limit time, the backup bypass operation to the public network is done to thereby enable the real-time communication to be further economically done.

In addition to the above-mentioned basic operations, MP (The PPP Multilink Protocol) is effective in order to reserve the stable quality of the communication that is easy and smooth, by solving the delay time and the packet loss in the real-time communication call induced in the backup switching or returning back operation when the trouble is induced in the IP (Internet) network 100, and then the normal state is recovered.

In the method for carrying out a real-time backup communication of IP communication according to the present invention, if the IP trouble is induced and the delay time is induced to the extent that the quality of the real-time communication can not be secured, it is treated as the real-time communication trouble, and the backup switching bypass operation can be automatically done to the public network 110. Moreover, in addition to the economically-large effect of enabling the real-time communication that is stable and high in quality on the very economical IP, although it is low in reliability and quality. So, this method can provide the largely economical effect that even a

low-grade maintainer, namely, a maintainer holding another typical service can carry out the maintenance operation without stationing a maintainer having high skill, and can quickly specify the trouble point and reduce the recovery time. Thus, it can improve the quality of the communication service and obtain the economical effect.

While the present invention has been described in its preferred embodiments, it is to be understood that the words which have been used are words of description rather than limitation, and that changes may be made to the invention without departing from its scope as defined by the appended claims.

Each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features.

The text of the abstract filed herewith is repeated here as part of the specification.

A method for detecting an occurrence of trouble in a real-time communication on an IP network through which a transmission-side node and a reception-side node are connected, and automatically bypassing a communication call of the real-time communication performed between the transmission-side node and the reception-side node from an IP network to a public network, based on the detecting result. Such a bypass operation enables the continuation of the real-

time communication. The occurrence of the trouble implies an occurrence of a delay time to an extent that the quality of the real-time communication cannot be secured. ICMP may be used in a periodical transmission/reception. There may be a case that the real-time communication call is newly-generated during the course of the real-time communication on the public network. In such a case, this makes even the new real-time communication go around the public network to thereby enable the real-time communication. If the trouble is recovered, the real-time communication is returned from the public network to the IP network. Thus, it is possible to avoid a drop of communication quality, caused by the network delay time and the network trouble in the economical Internet network, by using a cheap and simple method.

CLAIMS:

1. A method for carrying out a real-time backup communication of Internet Protocol (IP) communication, said method comprising the steps of:

detecting when the duration of a delay time, extending from transmission of an echo request message from a transmission-side node to reception of an echo answer message at the transmission-side node, exceeds a predetermined allowed time interval indicative of secured quality of a real-time communication on an IP network;

bypassing, depending on a result of the detecting step, from said IP network to a public network, a communication call of said real-time communication performed between said transmission-side node and said reception-side node; and,

bypassing a new communication call that occurs while said bypassing operation of said communication call to said public network is being performed.

2. A method according to claim 1, further comprising the step of judging, after the detected duration of the delay time has exceeded the predetermined allowed time, whether said IP network or said reception-side node is abnormal.

3. A method according to claim 1, further comprising the step of detecting an error in a real-time communication on said public network through which said transmission-side

node and said reception-side node are connected, said further step comprising detecting, on said public network, a duration of a delay time from a transmission of an echo request message to a reception of an echo answer message between said transmission-side node and said reception-side node.

4. A method according to claim 1, further comprising the step of detecting an error in a real-time communication on said public network through which said transmission-side node and said reception-side node are connected, said further step comprising judging, after the detected duration of a delay time for response to an echo request message has exceeded a predetermined allowed time interval for response to said message, whether said public network is abnormal.

5. A method according to claim 1, further comprising the step of judging whether it is the reception-side node that is abnormal or the IP network that is abnormal, the judgment being based on measuring the delay time for an echo signal passed along the public network after the communication call has been bypassed to the public network from the IP network.

6. A method according to any one of the preceding claims, wherein Internet Control Message Protocol (ICMP) is used in said transmission of said echo request message and reception of said echo answer message.

7. A system configured to effect the method of any one of claims 1 to 6.

8. A method for carrying out a real-time backup communication that includes one step of bypassing a communication call from an IP network to a public network and another step of bypassing a new communication call while the one step is being performed, the method being substantially as herein described with reference to, and as shown in, Figures 1 to 10 of the accompanying drawings.